ABSTRACT OF THE DISCLOSURE

An optimized approach for arriving at a shared secret key in a dynamically changing multicast or broadcast group environment is disclosed. In one aspect of the invention, a method is provided for communicating through a secure channel between members of a dynamically changing multicast group connected over an insecure network. The method provides that a first shared secret key for establishing a first multicast group is computed that includes a set of one or more first members. Based on the first shared secret key, a first multicast group exchange key is also generated. Upon receiving a first user exchange key from a first user requesting entry into the first multicast group, a second secret key, based on the first user exchange key and the first shared secret key is computed. The first multicast group exchange key is sent to the first user and used by the first user to generate the same second shared secret key. Through the use of the second shared secret key a second multicast group is established whose members include the first user and the set of one or more first members of the first multicast group as the second shared secret key provides a first secure channel for communicating between members of the second multicast group over the insecure network.